* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] An entrance check means to be the electronic equipment managerial system which manages utilization of the electronic equipment which the user who was installed into the chamber and entered this chamber uses, and to check that said user has entered the chamber concerned normally at the inlet port of said chamber, When the user who entered said chamber detects having started actuation of said electronic equipment and refers to the check result of said entrance check means When it is judged that the user concerned has entered a room normally with a decision means to judge whether the user concerned has entered a room normally, and this decision means, The electronic equipment managerial system characterized by providing the control means which refuses utilization of the electronic equipment concerned when it is judged that utilization of the electronic equipment concerned is permitted and the user concerned has not entered a room normally.
[Claim 2] An entrance check means to be the electronic equipment managerial system which manages utilization of the electronic equipment which the user who was installed into the chamber and entered this chamber uses, and to check that said user has entered the chamber concerned normally at the inlet port of said chamber, When it is checked by individual check means to check whether you are a just user in said electronic equipment, and this individual check means that he is a just user, by referring to the check result of said entrance check means When it is judged that the user concerned has entered a room normally with a decision means to judge whether the user concerned has entered a room normally, and this decision means, The electronic equipment managerial system characterized by providing the control means which refuses utilization of the electronic equipment concerned when it is judged that utilization of the electronic equipment concerned is permitted and the user concerned has not entered a room normally.
[Claim 3] Said electronic equipment is an electronic equipment managerial system according to claim 1 or 2 characterized by more than one existing.
[Claim 4] Said control means is an electronic equipment managerial system according to claim 1 or 2 characterized by what is reported while recording the result when utilization of the electronic equipment concerned is refused.
[Claim 5] For said entrance check means, said individual check means is an electronic equipment managerial system according to claim 2 characterized by using a different symptom.
[Claim 6] It is what the user who was installed into the chamber and entered this chamber uses. An entrance check means for each to be the electronic equipment managerial system which manages utilization of two or more computers equipped with the log in function manager, and to check that said user has entered the chamber concerned normally at the inlet port of said chamber, When the user who entered said chamber detects having started the log in to said computer and refers to the check result of said entrance check means When it is judged that the user concerned has entered a room normally with a decision means to judge whether the user concerned has entered a room normally, and this decision means, The electronic equipment managerial system characterized by

providing the control means which refuses a log in to the computer concerned when it is judged that a log in to the computer concerned is permitted and the user concerned has not entered a room normally.

[Claim 7] It is what the user who was installed into the chamber and entered this chamber uses. An entrance check means for each to be the electronic equipment managerial system which manages utilization of two or more computers equipped with the log in function manager, and to check that said user has entered the chamber concerned normally at the inlet port of said chamber, When it is checked in said two or more computers by individual check means to check whether you are a respectively just user, and this individual check means that he is a just user, by referring to the check result of said entrance check means When it is judged that the user concerned has entered a room normally with a decision means to judge whether the user concerned has entered a room normally, and this decision means, The electronic equipment managerial system characterized by providing the control means which refuses a log in to the computer concerned when it is judged that a log in to the computer concerned is permitted and the user concerned has not entered a room normally.

[Claim 8] The step which is the electronic equipment management method which manages utilization of the electronic equipment which the user who was installed into the chamber and entered this chamber uses, and checks that said user has entered the chamber concerned normally at the inlet port of said chamber, When the user who entered said chamber detects having started actuation of said electronic equipment and refers to the check result of said entrance into a room The step which judges whether the user concerned has entered a room normally, and when it is judged that the user concerned has entered a room normally by this decision, The electronic equipment management method characterized by providing the step which refuses utilization of the electronic equipment concerned when it is judged that utilization of the electronic equipment concerned is permitted and the user concerned has not entered a room normally.

[Claim 9] The step which is the electronic equipment management method which manages utilization of the electronic equipment which the user who was installed into the chamber and entered this chamber uses, and checks that said user has entered the chamber concerned normally at the inlet port of said chamber, The step which checks whether you are a just user in said electronic equipment, and by referring to the check result of said entrance into a room, when it is checked according to this check that he is a just user The step which judges whether the user concerned has entered a room normally, and when it is judged that the user concerned has entered a room normally by this decision, The electronic equipment management method characterized by providing the step which refuses utilization of the electronic equipment concerned when it is judged that utilization of the electronic equipment concerned is permitted and the user concerned has not entered a room normally.

[Claim 10] It is what the user who was installed into the chamber and entered this chamber uses. The step which each is the electronic equipment management method which manages utilization of two or more computers equipped with the log in function manager, and checks that said user has entered the chamber concerned normally at the inlet port of said chamber, When the user who entered said chamber detects having started the log in to said computer and refers to the check result of said entrance into a room The step which judges whether the user concerned has entered a room normally, and when it is judged that the user concerned has entered a room normally by this decision, The electronic equipment management method characterized by providing the step which refuses a log in to the computer concerned when it is judged that a log in to the computer concerned is permitted and the user concerned has not entered a room normally.

[Claim 11] It is what the user who was installed into the chamber and entered this chamber uses. The step which each is the electronic equipment management method which manages utilization of two or more computers equipped with the log in function manager, and checks that said user has entered the chamber concerned normally at the inlet port of said chamber, In said two or more

computers, the step which checks whether you are a respectively just user, and by referring to the check result of said entrance into a room, when it is checked according to this check that he is a just user The step which judges whether the user concerned has entered a room normally, and when it is judged that the user concerned has entered a room normally by this decision, The electronic equipment management method characterized by providing the step which refuses a log in to the computer concerned when it is judged that a log in to the computer concerned is permitted and the user concerned has not entered a room normally.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the electronic equipment managerial system and electronic equipment management method which manage utilization of electronic equipment, such as two or more computers and measuring machine machines which were installed into the chamber, and medical equipment.
[0002]
[Description of the Prior Art] In the usual office, in case a computer is used, the log in executive process (program) which operates by computer concerned They are delivery and a log in management server (as an example) to a log in management server about the login name and password which were entered from the screen. The form where a log in executive process permits access to a computer and the specified device for being [which were managed within the domain server] data and it having been in agreement after a carrier beam from a server is common in a Windows (trademark) network.
[0003] A login name and a password may always be stolen by the third party as it is this approach, and it may be used unjustly. Moreover, the object equipment of conditions which permits a log in is also performed based on logical data, such as a computer name and a network address.
[0004] in order to prevent unjust utilization on the other hand -- a principal -- although there is an approach using possession of an ID card and authentications (for example, fingerprint etc.) of a living body function as a means of a check, if it is necessary to add the reader and living body collating unit of an ID card for every computer and the installation number of a computer increases, in respect of cost, there will be many burdens and the actual condition will not have spread so much.
[0005] Moreover, at a general door, although unjust access is impossible by controlling access to a computer room by the mere close leaving system, since close leaving can be carried out with people with an access privilege, the actual condition does not become a perfect access control. If the door and door control which were prepared specially are used, such a phenomenon can be prevented to some extent, but since a pass takes time amount, it remains in a part of adoption very much.

[0006]
[Problem(s) to be Solved by the Invention] When performing personal authentication by the password and the personal identification number about access to a computer, even if it is controlling close leaving by the security device, the problem of the trespass by human being without entrance rating and the computer access by the member remains. Moreover, it will be in the condition of always being exposed to an inaccurate visitor's threat, also in free close leaving in a location and the combination of a personal authentication device (fingerprint authentication and ID card) without close leaving control.
[0007] Especially, in the conventional log in management, a partner can be specified only by logical data, and physical constraint cannot be applied, but it is always exposed to the possibility of hacking from the others.
[0008] furthermore, an approach independent at the time of a log in to a computer -- a principal -- when checking and it has broken through the wall with a certain means, a check will not start after it but access will be allowed freely.
[0009] Then, this invention can eliminate utilization of the electronic equipment by trespass of people without entrance authorization, and aims at offering the electronic equipment managerial system and electronic equipment management method which can raise security remarkably.
[0010]
[Means for Solving the Problem] It is the electronic equipment managerial system which manages utilization of the electronic equipment which the user who the electronic equipment managerial system of this invention was installed into the chamber, and entered this chamber uses. An entrance check means to check that said user has entered the chamber concerned normally at the inlet port of said chamber, When the user who entered said chamber detects having started actuation of said electronic equipment and refers to the check result of said entrance check means When it is judged that the user concerned has entered a room normally with a decision means to judge whether the user concerned has entered a room normally, and this decision means, Utilization of the electronic equipment concerned is permitted, and when the user concerned is judged to have not entered a room normally, the control means which refuses utilization of the electronic equipment concerned is provided.
[0011] Moreover, it is the electronic equipment managerial system which manages utilization of the electronic equipment which the user who the electronic equipment managerial system of this invention was installed into the chamber, and entered this chamber uses. An entrance check means to check that said user has entered the chamber concerned normally at the inlet port of said chamber, When it is checked by individual check means to check whether you are a just user in said electronic equipment, and this individual check means that he is a just user, by referring to the check result of said entrance check means When it is judged that the user concerned has entered a room normally with a decision means to judge whether the user concerned has entered a room normally, and this decision means, Utilization of the electronic equipment concerned is permitted, and when the user concerned is judged to have not entered a room normally, the control means which refuses utilization of the electronic equipment concerned is provided.
[0012] Moreover, it is what the user who the electronic equipment managerial system of this invention was installed into the chamber, and entered this chamber uses. An entrance check means for each to be the electronic equipment managerial system which manages utilization of two or more computers equipped with the log in function manager, and to check that said user has entered the chamber concerned normally at the inlet port of said chamber, When the user who entered said chamber detects having started the log in to said computer and refers to the check result of said entrance check means When it is judged that the user concerned has entered a room normally with a decision means to judge whether the user concerned has entered a room normally, and this decision means, A log in to the computer concerned is permitted, and when the user concerned is judged to have not entered a room normally, the control means which refuses a log in to the

computer concerned is provided.
[0013] Moreover, it is what the user who the electronic equipment managerial system of this invention was installed into the chamber, and entered this chamber uses. An entrance check means for each to be the electronic equipment managerial system which manages utilization of two or more computers equipped with the log in function manager, and to check that said user has entered the chamber concerned normally at the inlet port of said chamber, When it is checked in said two or more computers by individual check means to check whether you are a respectively just user, and this individual check means that he is a just user, by referring to the check result of said entrance check means When it is judged that the user concerned has entered a room normally with a decision means to judge whether the user concerned has entered a room normally, and this decision means, A log in to the computer concerned is permitted, and when the user concerned is judged to have not entered a room normally, the control means which refuses a log in to the computer concerned is provided.
[0014] Moreover, it is the electronic equipment management method which manages utilization of the electronic equipment which the user who the electronic equipment management method of this invention was installed into the chamber, and entered this chamber uses. When the step which checks that said user has entered the chamber concerned normally at the inlet port of said chamber, and the user who entered said chamber detect having started actuation of said electronic equipment and refers to the check result of said entrance into a room The step which judges whether the user concerned has entered a room normally, and when it is judged that the user concerned has entered a room normally by this decision, Utilization of the electronic equipment concerned is permitted, and when the user concerned is judged to have not entered a room normally, the step which refuses utilization of the electronic equipment concerned is provided.
[0015] Moreover, it is the electronic equipment management method which manages utilization of the electronic equipment which the user who the electronic equipment management method of this invention was installed into the chamber, and entered this chamber uses. The step which checks that said user has entered the chamber concerned normally at the inlet port of said chamber, The step which checks whether you are a just user in said electronic equipment, and by referring to the check result of said entrance into a room, when it is checked according to this check that he is a just user The step which judges whether the user concerned has entered a room normally, and when it is judged that the user concerned has entered a room normally by this decision, Utilization of the electronic equipment concerned is permitted, and when the user concerned is judged to have not entered a room normally, the step which refuses utilization of the electronic equipment concerned is provided.
[0016] Moreover, it is what the user who the electronic equipment management method of this invention was installed into the chamber, and entered this chamber uses. The step which each is the electronic equipment management method which manages utilization of two or more computers equipped with the log in function manager, and checks that said user has entered the chamber concerned normally at the inlet port of said chamber, When the user who entered said chamber detects having started the log in to said computer and refers to the check result of said entrance into a room The step which judges whether the user concerned has entered a room normally, and when it is judged that the user concerned has entered a room normally by this decision, A log in to the computer concerned is permitted, and when the user concerned is judged to have not entered a room normally, the step which refuses a log in to the computer concerned is provided.
[0017] Moreover, it is what the user who the electronic equipment management method of this invention was installed into the chamber, and entered this chamber uses. The step which each is the electronic equipment management method which manages utilization of two or more computers equipped with the log in function manager, and checks that said user has entered the chamber concerned normally at the inlet port of said chamber, In said two or more computers, the step which checks whether you are a respectively just user, and by referring to the check result of said

entrance into a room, when it is checked according to this check that he is a just user The step which judges whether the user concerned has entered a room normally, and when it is judged that the user concerned has entered a room normally by this decision, A log in to the computer concerned is permitted, and when the user concerned is judged to have not entered a room normally, the step which refuses a log in to the computer concerned is provided.
[0018] According to this invention, at the time of a log in to a computer, for example on the conditions of a log in The conditions by the entrance check means using an ID card, fingerprint authentication, etc. that the user has entered the chamber in which the computer concerned was installed normally are added and judged. By permitting a log in, only when having entered a room normally, and refusing a log in, when having not entered a room normally, a log in to the computer by trespass of people without entrance authorization can be eliminated, and security can be raised remarkably.
[0019]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to a drawing.
[0020] First, the gestalt of the 1st operation is explained.
[0021] Drawing 1 shows the configuration of the electronic equipment managerial system concerning the gestalt of the 1st operation. The usual office environment is assumed and, as for drawing 1 , two or more client (for general) computers 4 connected with the log in management server 2 through the network 3 and -- are installed in office (chamber) 1. In addition, each computer 4 shall be equipped with a log in function manager (log in executive process).
[0022] Moreover, while the close leaving registration equipment 7 the close leaving management server 6 and for data registration (terminal computer) connected through the network 5 as a close leaving managerial system is installed, it is installed in the gate 8 of office 1, and the entrance-into-a-room side control unit 9 as a close leaving control unit which performs control of authorization/disapproval of close leaving, and an electric lock, and the leaving side control unit 10 are formed. It connects through a hub 11 and a network 3 and a network 5 can communicate by mutual.
[0023] In addition, although the body descriptions, such as a case where ID cards, such as a wireless type ID card and a magnetic card, are used, and fingerprint authentication, may generally be used for a close leaving control unit, the either may not specify but may use any here.
[0024] Although these two systems (close leaving management and log in management) have the common case where it exists independently, under such a situation, the access prevention to the computer for general of those who passed through close leaving management and have entered a room will become only a login name and a personal identification number.
[0025] With the gestalt of this operation, the server of these two systems is mutually connected through a network (the hub 11 in drawing 1 is equivalent to it), and it is further characterized by adding the normal entrance into a room (to the chamber concerned) by close leaving management as conditions for a log in.
[0026] Next, it explains, referring to the flow chart shown in drawing 2 about the actuation at the time of a fundamental log in.
[0027] First, registration of the person (user) who can enter this chamber (office 1) is beforehand performed to the entrance-into-a-room side control unit 9 and the leaving side control unit 10 via the close leaving management server 6 from close leaving registration equipment 7, respectively. If registered in the case of an ID card, in the case of an ID number and fingerprint authentication, it will be a principal's data for fingerprint authentication.
[0028] Now, suppose that Mr. A to whom entrance into a room was permitted now entered office 1. The judgment result of the entrance authorization is sent to the close leaving management server 6 from the entrance-into-a-room side control device 9, and Mr. A is remembered to be a normal entrance-into-a-room condition in office 1. Then, if it is going to log in by Mr. A inputting a login

name from the predetermined computer 4 in office 1, by detecting it, the log in executive process in a computer 4 (program) will go [whether it is in a normal entrance-into-a-room condition, and] to the chamber (here office 1) where an own computer has those who have the login name concerned in the close leaving management server 6 to check rather than will go to the direct log in management server 2 to attest.

[0029] Since Mr. A's login name is beforehand matched with Mr. A and is registered into the close leaving management server 6, Mr. A is searched from the login name, and, specifically, Mr. A's close leaving condition is searched. In addition, suppose that the information on in which chamber it is installed is made to memorize beforehand, or an installation name is added to a computer name into a computer 4. From this information, if a log in executive process is in a normal entrance-into-a-room condition, it will request log in processing from the office 1 in which the computer 4 is installed to the log in management server 2 as a following step. Here, a login name and a password (personal identification number) are checked, and if the content is right, a log in will be permitted normally.

[0030] If Mr. A logs out by finishing an activity, a log in executive process will request log out processing to the log in management server 2 by detecting it. Next, if Mr. A leaves a room, leaving information is sent to the close leaving management server 6 from the leaving side control device 10, and Mr. A's condition will be in a leaving condition.

[0031] Here, although a log in executive process will go Mr. A's close leaving condition to the close leaving management server 6 to check first as described above if the another person who entered injustice receives Mr. A's login name and password and tries a log in, since Mr. A is in a leaving condition in this case, it will not go but can log in to the processing to the following log in management server 2. That is, a log in to a computer 4 is refused.

[0032] If the attempt of such an unjust log in is performed, the alarm display of it will be carried out by display 6a of the close leaving management server 6, and warning will be urged to it while a log in executive process notifies that to the close leaving management server 6 and leaves it as record in the close leaving management server 6.

[0033] Next, the gestalt of the 2nd operation is explained.

[0034] With the gestalt of the 1st operation mentioned above, although the log in executive process in a computer 4 checked the close leaving condition to the close leaving management server 6, the log in executive process in the log in management server 2 is made to check the close leaving condition to the close leaving management server 6, and the gestalt of the 2nd operation shows the flow of the actuation to the flow chart of drawing 3 . In this case, without completely changing a motion of the log in executive process of a computer 4, it realizes because a user's close leaving condition which is judged from a login name in addition to the registered general login name, and a password and a computer name checks that it is in a normal entrance-into-a-room condition as conditions for log in authorization of a request of a log in of the log in executive process in the carrier beam log in management server 2, and others are the same as that of the gestalt of the 1st operation.

[0035] Next, the gestalt of the 3rd operation is explained.

[0036] Drawing 4 shows the configuration of the electronic equipment managerial system concerning the gestalt of the 3rd operation. A different point from the gestalt of the 1st operation which the gestalt of the 3rd operation mentioned above is in the point of having installed the individual check equipment (thing using a fingerprint collation device if it is an ID card and is the thing and fingerprint using ID card reader) 12 which checks whether you being a respectively just user not only to the gate 8 of office 1 but to each computer 4, and others are the same as that of the gestalt of the 1st operation. In this case, the combination of a different symptom from the close leaving control devices 9 and 10 installed in the gate 8 is effective in the semantics which secures higher security. For example, the close leaving control unit of a gate 8 uses the symptom according [the individual check equipment 12 for every computer 4] to fingerprint authentication using the symptom by the ID card.

[0037] The flow of actuation in the case of the gestalt of this 3rd operation is shown in the flow chart of drawing 5 . In this case, the log in executive process by the side of a computer 4 After checking whether the principal itself has accessed by using individual check equipment 12, Information (for example, ID number the significance [ID number] was given by fingerprint information and 1 to 1 when it was an ID card and was an ID number and fingerprint authentication) which specifies the individual read in individual check equipment 12 is made into a login name. Only when an entrance condition is asked to the close leaving management server 6 and a normal entrance-into-a-room condition is suited, log in processing is requested to the log in management server 2.
[0038] In addition, in the case of fingerprint authentication, a part or all of fingerprint information may be used for the password (personal identification number) used with individual check equipment 12, using the input from a keyboard.
[0039] Thus, when processing is added to the log in executive process by the side of a computer 4, it is not necessary to add a hand to the program of the existing log in management server 2, and there is an advantage which can strengthen a system simple. Moreover, since the computer access from the chamber which does not have entrance authorization by checking a close leaving condition can be forbidden, it becomes possible to add the physical limit of the location to access.
[0040] Furthermore, even when it breaks through individual check equipment 12 with an unjust means by a certain approach in this case, an unjust log in can be beforehand prevented by checking further the data by the side of close leaving management.
[0041] At the time of a log in to two or more computers 4 which were installed in office 1 according to the gestalt of the above-mentioned implementation as explained above Are based on the entrance-into-a-room side control unit 9 which used an ID card, fingerprint authentication, etc. for the conditions of a log in. By a user adding and judging the conditions of having entered a room in the office 1 in which the computer 4 concerned was installed normally, permitting a log in, only when having entered a room normally, and refusing a log in, when having not entered a room normally It becomes possible to eliminate a log in to the computer 4 by trespass of people without entrance authorization. Moreover, a physical location is pinpointed and a limit of the log in from a computer 4 is attained. Moreover, even when there is no device for an individual check in each computer 4, the above-mentioned operation effectiveness can be realized cheaply. Furthermore, it is effective in heightening the effectiveness of unjust access prevention more by combining two or more identification.
[0042] In addition, although the gestalt of said operation explained the case where utilization of two or more computers installed in office was managed, this invention is not limited to this, and when managing [for example,] utilization of other electronic equipment, such as a measuring machine machine and medical equipment, it can be applied similarly.
[0043]
[Effect of the Invention] As explained in full detail above, utilization of the electronic equipment by trespass of those who do not have entrance authorization according to this invention can be eliminated, and the electronic equipment managerial system and electronic equipment management method which can raise security remarkably can be offered.

[Translation done.]

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

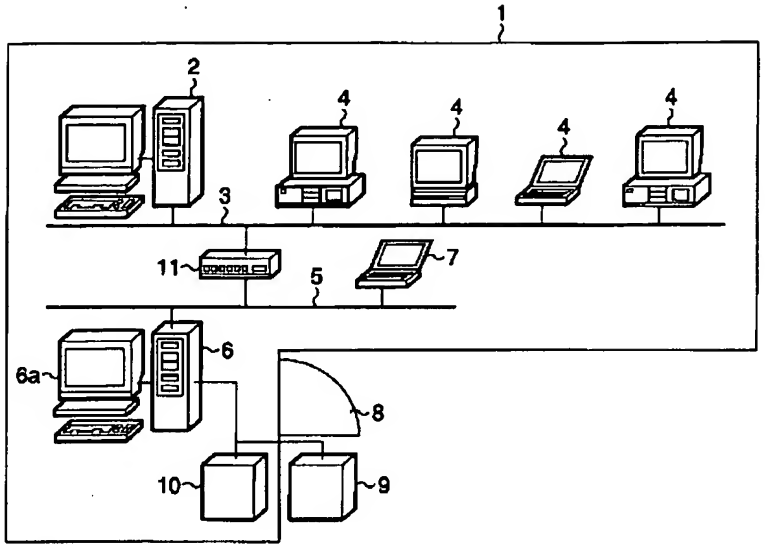
[Brief Description of the Drawings]
[Drawing 1] The block diagram showing typically the configuration of the electronic equipment managerial system concerning the gestalt of operation of the 1st of this invention.
[Drawing 2] The flow chart explaining the actuation at the time of the fundamental log in concerning the gestalt of the 1st operation.
[Drawing 3] The flow chart explaining the actuation at the time of the fundamental log in concerning the gestalt of the 2nd operation.
[Drawing 4] The block diagram showing typically the configuration of the electronic equipment managerial system concerning the gestalt of operation of the 3rd of this invention.
[Drawing 5] The flow chart explaining the actuation at the time of the fundamental log in concerning the gestalt of the 3rd operation.
[Description of Notations]
1 -- Office (chamber)
2 -- Log in management server
4 -- Computer (electronic equipment)
6 -- Close leaving management server
7 -- Close leaving registration equipment
8 -- Gate
9 -- Entrance-into-a-room side control unit
10 -- Leaving side control unit
12 -- Individual check equipment

[Translation done.]

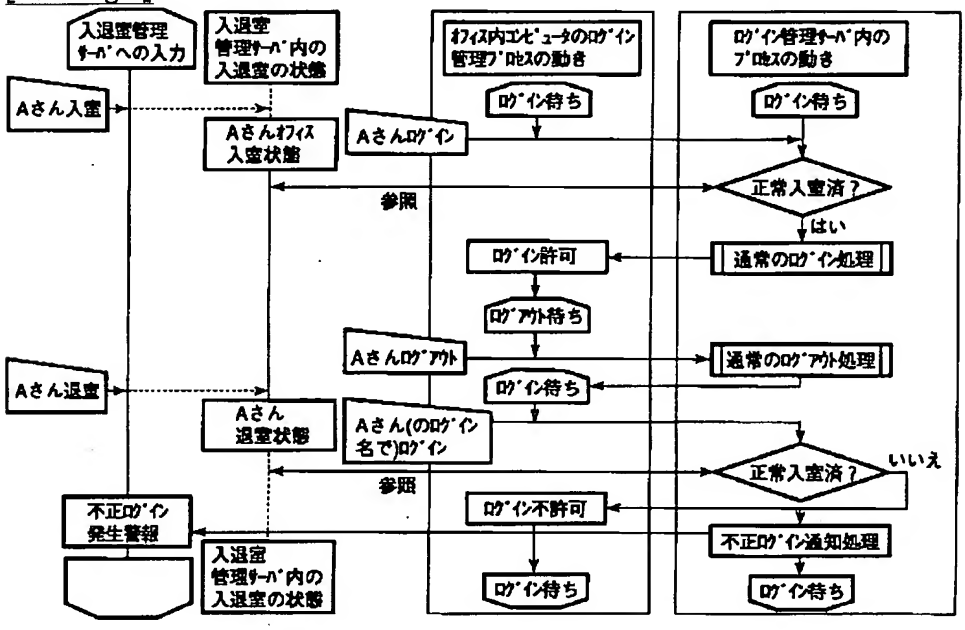
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

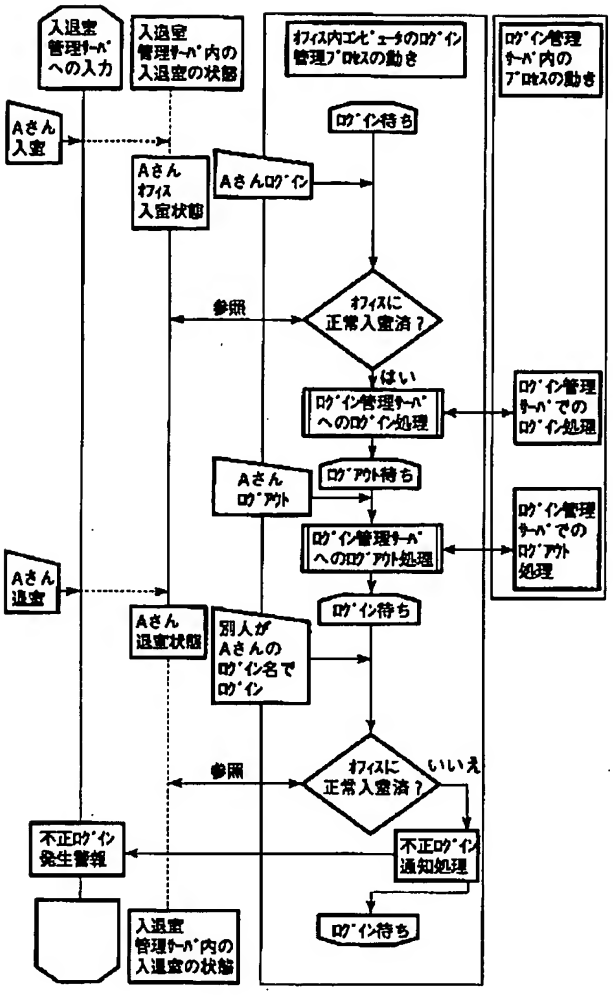
[Drawing 1]



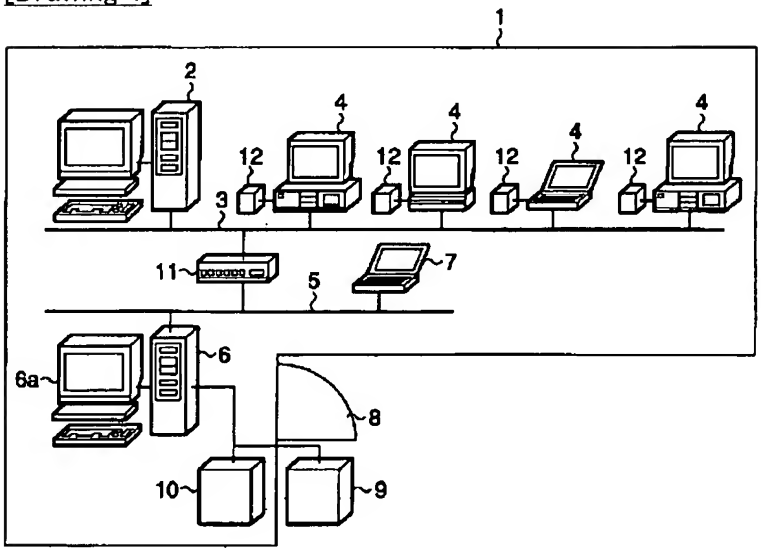
[Drawing 3]



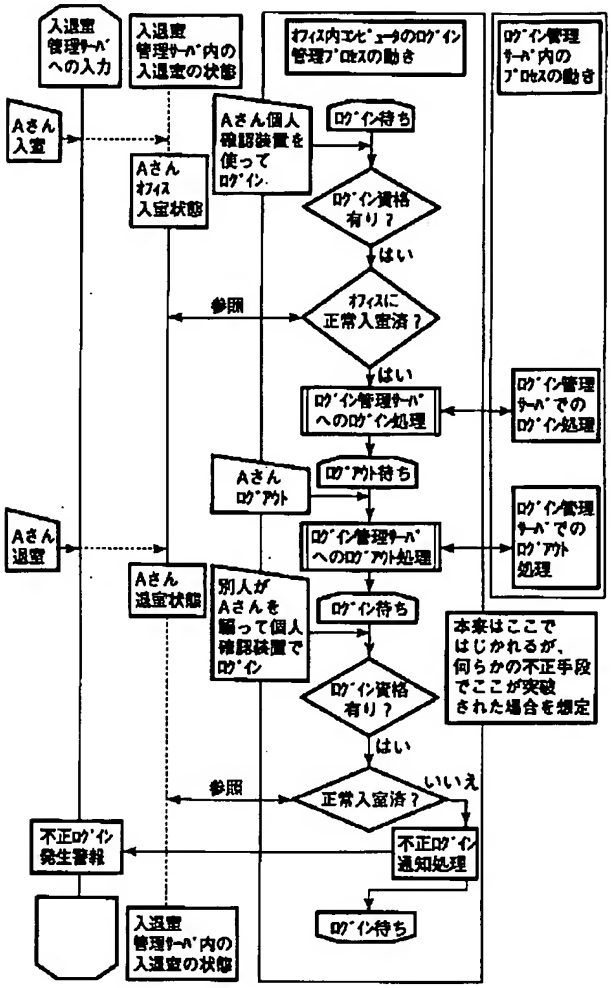
[Drawing 2]



[Drawing 4]



[Drawing 5]



[Translation done.]

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-041469**
(43)Date of publication of application : **08.02.2002**

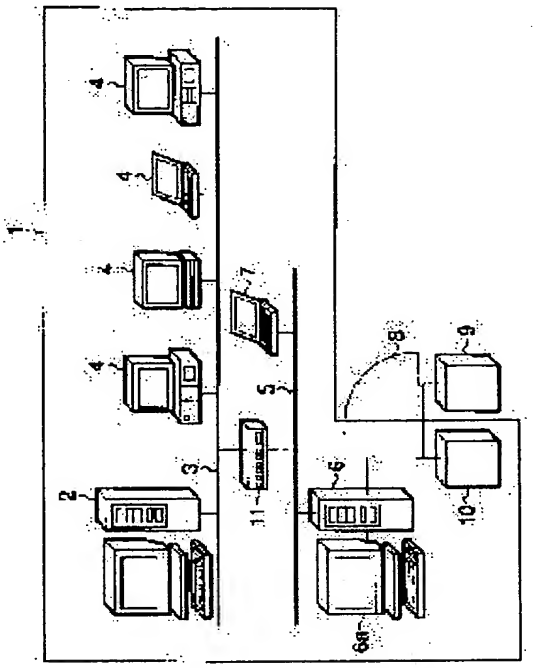
(51)Int.Cl. **G06F 15/00**

(21)Application number : **2000-221181**
(22)Date of filing : **21.07.2000**

(71)Applicant : **TOSHIBA CORP**
(72)Inventor : **TAKAGI KAZUYOSHI**

(54) SYSTEM AND METHOD FOR MANAGING ELECTRONIC EQUIPMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an electronic equipment management system and an electronic equipment managing method, capable of preventing a person who is not allowed to enter the office from intruding and using electronic equipment, and improving security to a high level.
SOLUTION: When a plurality of computers 4 installed in an office 1, an entrance side controller 9 using an IC card, fingerprint matching, etc., makes a decision, while a condition that a user normally is in the office 1 where the computers 4 are installed is added to the condition of login, logging in to the computers 4 is allowed, only when the user normally in the office, and the logging in to the computers 4 is rejected, when the user has not entered the office 1 in the normal manner.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－41469
（P2002－41469A）
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ　５Ｂ０８５

審査請求　未請求　請求項の数11　ＯＬ　（全８頁）

(21)出願番号　特願2000－221181(P2000－221181)

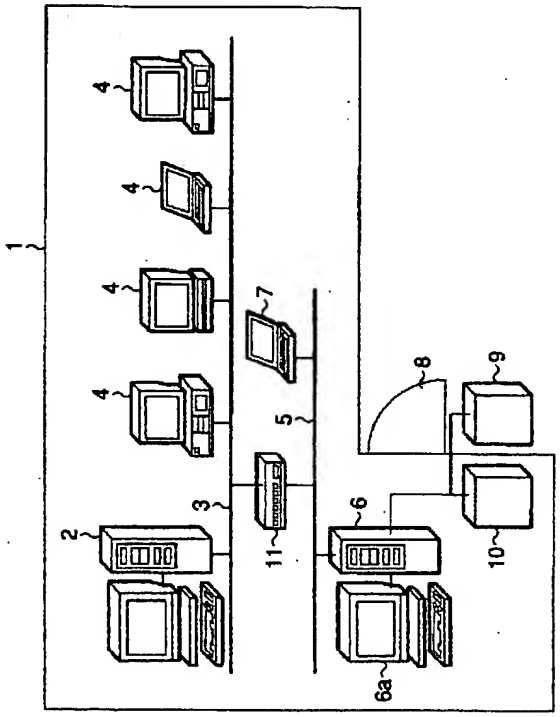
(22)出願日　平成12年７月21日(2000.7.21)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　高木　一圭
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町事業所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5B085 BC01

(54)【発明の名称】　電子機器管理システムおよび電子機器管理方法

(57)【要約】
【課題】入室許可のない人の侵入による電子機器の利用を排除することができ、セキュリティを著しく向上させることができる電子機器管理システムおよび電子機器管理方法を提供する。
【解決手段】オフィス１内に設置された複数のコンピュータ４へのログイン時、ログインの条件に、ＩＤカードや指紋照合などを用いた入室側制御装置９による、利用者が正常に当該コンピュータ４の設置されたオフィス１内に入室しているという条件を加えて判断し、正常に入室している場合にだけ当該コンピュータ４へのログインを許可し、正常に入室していない場合には当該コンピュータ４へのログインを拒否する。



【特許請求の範囲】
【請求項１】　部屋の中に設置され、この部屋に入室した利用者が利用する電子機器の利用を管理する電子機器管理システムであって、
前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認する入室確認手段と、
前記部屋に入室した利用者が前記電子機器の操作を開始したことを検知し、前記入室確認手段の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断する判断手段と、
この判断手段により当該利用者が正常に入室していると判断された場合、当該電子機器の利用を許可し、当該利用者が正常に入室していないと判断された場合、当該電子機器の利用を拒否する制御手段と、
を具備したことを特徴とする電子機器管理システム。
【請求項２】　部屋の中に設置され、この部屋に入室した利用者が利用する電子機器の利用を管理する電子機器管理システムであって、
前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認する入室確認手段と、
前記電子機器において正当な利用者であるか否かを確認する個人確認手段と、この個人確認手段により正当な利用者であると確認された場合、前記入室確認手段の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断する判断手段と、
この判断手段により当該利用者が正常に入室していると判断された場合、当該電子機器の利用を許可し、当該利用者が正常に入室していないと判断された場合、当該電子機器の利用を拒否する制御手段と、
を具備したことを特徴とする電子機器管理システム。
【請求項３】　前記電子機器は複数個存在することを特徴とする請求項１または請求項２記載の電子機器管理システム。
【請求項４】　前記制御手段は、当該電子機器の利用を拒否した場合、その結果を記録するとともに報知することを特徴とする請求項１または請求項２記載の電子機器管理システム。
【請求項５】　前記個人確認手段は前記入室確認手段とは異なる確認方法を用いることを特徴とする請求項２記載の電子機器管理システム。
【請求項６】　部屋の中に設置され、この部屋に入室した利用者が利用するもので、それぞれがログイン管理機能を備えた複数のコンピュータの利用を管理する電子機器管理システムであって、
前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認する入室確認手段と、
前記部屋に入室した利用者が前記コンピュータへのログインを開始したことを検知し、前記入室確認手段の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断する判断手段と、
この判断手段により当該利用者が正常に入室していると判断された場合、当該コンピュータへのログインを許可し、当該利用者が正常に入室していないと判断された場合、当該コンピュータへのログインを拒否する制御手段と、
を具備したことを特徴とする電子機器管理システム。
【請求項７】　部屋の中に設置され、この部屋に入室した利用者が利用するもので、それぞれがログイン管理機能を備えた複数のコンピュータの利用を管理する電子機器管理システムであって、
前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認する入室確認手段と、
前記複数のコンピュータにおいて、それぞれ正当な利用者であるか否かを確認する個人確認手段と、
この個人確認手段により正当な利用者であると確認された場合、前記入室確認手段の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断する判断手段と、
この判断手段により当該利用者が正常に入室していると判断された場合、当該コンピュータへのログインを許可し、当該利用者が正常に入室していないと判断された場合、当該コンピュータへのログインを拒否する制御手段と、
を具備したことを特徴とする電子機器管理システム。
【請求項８】　部屋の中に設置され、この部屋に入室した利用者が利用する電子機器の利用を管理する電子機器管理方法であって、
前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認するステップと、
前記部屋に入室した利用者が前記電子機器の操作を開始したことを検知し、前記入室の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断するステップと、
この判断により当該利用者が正常に入室していると判断された場合、当該電子機器の利用を許可し、当該利用者が正常に入室していないと判断された場合、当該電子機器の利用を拒否するステップと、
を具備したことを特徴とする電子機器管理方法。
【請求項９】　部屋の中に設置され、この部屋に入室した利用者が利用する電子機器の利用を管理する電子機器管理方法であって、
前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認するステップと、
前記電子機器において正当な利用者であるか否かを確認するステップと、
この確認により正当な利用者であると確認された場合、前記入室の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断するステップと、
この判断により当該利用者が正常に入室していると判断された場合、当該電子機器の利用を許可し、当該利用者

が正常に入室していないと判断された場合、当該電子機器の利用を拒否するステップと、
を具備したことを特徴とする電子機器管理方法。
【請求項１０】　部屋の中に設置され、この部屋に入室した利用者が利用するもので、それぞれがログイン管理機能を備えた複数のコンピュータの利用を管理する電子機器管理方法であって、
前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認するステップと、
前記部屋に入室した利用者が前記コンピュータへのログインを開始したことを検知し、前記入室の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断するステップと、
この判断により当該利用者が正常に入室していると判断された場合、当該コンピュータへのログインを許可し、当該利用者が正常に入室していないと判断された場合、当該コンピュータへのログインを拒否するステップと、
を具備したことを特徴とする電子機器管理方法。
【請求項１１】　部屋の中に設置され、この部屋に入室した利用者が利用するもので、それぞれがログイン管理機能を備えた複数のコンピュータの利用を管理する電子機器管理方法であって、
前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認するステップと、
前記複数のコンピュータにおいて、それぞれ正当な利用者であるか否かを確認するステップと、
この確認により正当な利用者であると確認された場合、前記入室の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断するステップと、
この判断により当該利用者が正常に入室していると判断された場合、当該コンピュータへのログインを許可し、当該利用者が正常に入室していないと判断された場合、当該コンピュータへのログインを拒否するステップと、
を具備したことを特徴とする電子機器管理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、たとえば、部屋の中に設置された複数のコンピュータや計測機器、医療機器などの電子機器の利用を管理する電子機器管理システムおよび電子機器管理方法に関する。
【０００２】
【従来の技術】通常のオフィスでは、コンピュータを利用する際に、当該コンピュータで動作するログイン管理プロセス（プログラム）が、画面から入力されたログイン名とパスワードをログイン管理サーバに送り、ログイン管理サーバ（例として、ウインドウズ（登録商標）ネットワークではドメインサーバ）内で管理されたデータと、それが一致したことをサーバから受けた後に、ログイン管理プロセスがコンピュータおよび指定された機器へのアクセスを許可するという形が一般的である。
【０００３】この方法であると、常にログイン名とパスワードを第三者に盗まれ、不正に利用される可能性がある。また、ログインを許可する条件の対象装置も、コンピュータ名やネットワークアドレスなどの論理的データを基に行なわれている。
【０００４】一方、不正利用を防ぐために、本人確認の手段として、ＩＤカードの所持、生体機能の認証（たとえば、指紋など）を用いる方法があるが、コンピュータごとにＩＤカードの読取装置や、生体照合装置を付加する必要があり、コンピュータの設置台数が多くなるとコストの点で負担が多く、それほど普及していないのが実情である。
【０００５】また、単なる入退室システムで、コンピュータルームへのアクセスを制御することにより、不正なアクセスは不可能であるが、一般のドアではアクセス権のある人とともに入退室できてしまうために、完全なアクセス制御にならないのが実情である。特別に用意されたドアおよびドア制御を用いれば、このような現象をある程度防止できるが、通行に時間がかかるため、ごく一部の採用にとどまっている。
【０００６】
【発明が解決しようとする課題】コンピュータへのアクセスに関して、個人認証をパスワードと暗証番号とで行なう場合は、入退室をセキュリティ機器で制御していても、入室資格のない人間による侵入および同人によるコンピュータアクセスの問題が残る。また、入退室制御のない場所でのフリーな入退室と個人認証機器（指紋照合やＩＤカード）の組み合わせでも、不正入場者の脅威に常にさらされている状態になる。
【０００７】特に、従来のログイン管理では、論理的なデータでしか相手を特定できず、物理的な制約をかけられず、他者からのハッキングの可能性に常にさらされている。
【０００８】さらに、コンピュータへのログイン時に、単独の方法で本人確認を行なっている場合、なんらかの手段でその壁を突破してしまった場合、それ以後にチェックがかからず、自由にアクセスを許してしまうことになる。
【０００９】そこで、本発明は、入室許可のない人の侵入による電子機器の利用を排除することができ、セキュリティを著しく向上させることができる電子機器管理システムおよび電子機器管理方法を提供することを目的とする。
【００１０】
【課題を解決するための手段】本発明の電子機器管理システムは、部屋の中に設置され、この部屋に入室した利用者が利用する電子機器の利用を管理する電子機器管理システムであって、前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認する入室確認手段と、前記部屋に入室した利用者が前記電子機器の操作

を開始したことを検知し、前記入室確認手段の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断する判断手段と、この判断手段により当該利用者が正常に入室していると判断された場合、当該電子機器の利用を許可し、当該利用者が正常に入室していないと判断された場合、当該電子機器の利用を拒否する制御手段とを具備している。

【００１１】また、本発明の電子機器管理システムは、部屋の中に設置され、この部屋に入室した利用者が利用する電子機器の利用を管理する電子機器管理システムであって、前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認する入室確認手段と、前記電子機器において正当な利用者であるか否かを確認する個人確認手段と、この個人確認手段により正当な利用者であると確認された場合、前記入室確認手段の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断する判断手段と、この判断手段により当該利用者が正常に入室していると判断された場合、当該電子機器の利用を許可し、当該利用者が正常に入室していないと判断された場合、当該電子機器の利用を拒否する制御手段とを具備している。

【００１２】また、本発明の電子機器管理システムは、部屋の中に設置され、この部屋に入室した利用者が利用するもので、それぞれがログイン管理機能を備えた複数のコンピュータの利用を管理する電子機器管理システムであって、前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認する入室確認手段と、前記部屋に入室した利用者が前記コンピュータへのログインを開始したことを検知し、前記入室確認手段の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断する判断手段と、この判断手段により当該利用者が正常に入室していると判断された場合、当該コンピュータへのログインを許可し、当該利用者が正常に入室していないと判断された場合、当該コンピュータへのログインを拒否する制御手段とを具備している。

【００１３】また、本発明の電子機器管理システムは、部屋の中に設置され、この部屋に入室した利用者が利用するもので、それぞれがログイン管理機能を備えた複数のコンピュータの利用を管理する電子機器管理システムであって、前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認する入室確認手段と、前記複数のコンピュータにおいて、それぞれ正当な利用者であるか否かを確認する個人確認手段と、この個人確認手段により正当な利用者であると確認された場合、前記入室確認手段の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断する判断手段と、この判断手段により当該利用者が正常に入室していると判断された場合、当該コンピュータへのログインを許可し、当該利用者が正常に入室していないと判断された場合、当該コンピュータへのログインを拒否する制御手段とを具備している。

【００１４】また、本発明の電子機器管理方法は、部屋の中に設置され、この部屋に入室した利用者が利用する電子機器の利用を管理する電子機器管理方法であって、前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認するステップと、前記部屋に入室した利用者が前記電子機器の操作を開始したことを検知し、前記入室の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断するステップと、この判断により当該利用者が正常に入室していると判断された場合、当該電子機器の利用を許可し、当該利用者が正常に入室していないと判断された場合、当該電子機器の利用を拒否するステップとを具備している。

【００１５】また、本発明の電子機器管理方法は、部屋の中に設置され、この部屋に入室した利用者が利用する電子機器の利用を管理する電子機器管理方法であって、前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認するステップと、前記電子機器において正当な利用者であるか否かを確認するステップと、この確認により正当な利用者であると確認された場合、前記入室の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断するステップと、この判断により当該利用者が正常に入室していると判断された場合、当該電子機器の利用を許可し、当該利用者が正常に入室していないと判断された場合、当該電子機器の利用を拒否するステップとを具備している。

【００１６】また、本発明の電子機器管理方法は、部屋の中に設置され、この部屋に入室した利用者が利用するもので、それぞれがログイン管理機能を備えた複数のコンピュータの利用を管理する電子機器管理方法であって、前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認するステップと、前記部屋に入室した利用者が前記コンピュータへのログインを開始したことを検知し、前記入室の確認結果を参照することにより、当該利用者が正常に入室しているか否かを判断するステップと、この判断により当該利用者が正常に入室していると判断された場合、当該コンピュータへのログインを許可し、当該利用者が正常に入室していないと判断された場合、当該コンピュータへのログインを拒否するステップとを具備している。

【００１７】また、本発明の電子機器管理方法は、部屋の中に設置され、この部屋に入室した利用者が利用するもので、それぞれがログイン管理機能を備えた複数のコンピュータの利用を管理する電子機器管理方法であって、前記部屋の入口において前記利用者が当該部屋に正常に入室したことを確認するステップと、前記複数のコンピュータにおいて、それぞれ正当な利用者であるか否かを確認するステップと、この確認により正当な利用者であると確認された場合、前記入室の確認結果を参照することにより、当該利用者が正常に入室しているか否か

を判断するステップと、この判断により当該利用者が正常に入室していると判断された場合、当該コンピュータへのログインを許可し、当該利用者が正常に入室していないと判断された場合、当該コンピュータへのログインを拒否するステップとを具備している。

【００１８】本発明によれば、たとえば、コンピュータへのログイン時、ログインの条件に、ＩＤカードや指紋照合などを用いた入室確認手段による、利用者が正常に当該コンピュータの設置された部屋に入室しているという条件を加えて判断し、正常に入室している場合にだけログインを許可し、正常に入室していない場合にはログインを拒否することにより、入室許可のない人の侵入によるコンピュータへのログインを排除することができ、セキュリティを著しく向上させることができるものである。

【００１９】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【００２０】まず、第１の実施の形態について説明する。

【００２１】図１は、第１の実施の形態に係る電子機器管理システムの構成を示すものである。図１は、たとえば、通常のオフィス環境を想定しており、オフィス（部屋）１内には、ログイン管理サーバ２とネットワーク３を介して接続された複数のクライアント（一般用）コンピュータ４，…が設置されている。なお、各コンピュータ４は、ログイン管理機能（ログイン管理プロセス）を備えているものとする。

【００２２】また、入退室管理システムとして、ネットワーク５を介して接続された入退室管理サーバ６とデータ登録用の入退室登録装置（端末コンピュータ）７が設置されているとともに、オフィス１の出入口８に設置され、入退室の許可／不許可と電気錠の制御を行なう入退室制御装置としての入室側制御装置９および退室側制御装置１０が設けられている。ネットワーク３およびネットワーク５は、ハブ１１を介して接続され、相互で通信可能となっている。

【００２３】なお、入退室制御装置は、一般的には無線式ＩＤカードや磁気カードなどのＩＤカードを用いる場合や、指紋照合などの身体特徴を用いる場合などがあるが、ここではそのどちらかは特定せず、いずれを用いてもよい。

【００２４】これらの２つのシステム（入退室管理とログイン管理）は独立して存在する場合が一般的であるが、このような状況下では入退室管理をすり抜けて入室してしまった人の、一般用コンピュータへのアクセス防止は、ログイン名と暗証番号のみとなってしまう。

【００２５】本実施の形態では、これら２つのシステムのサーバをネットワークを介して相互に接続し（図１におけるハブ１１がそれに相当）、さらに、ログインのための条件として、入退室管理での正常入室（当該部屋への）を付加することを特徴としている。

【００２６】次に、基本的なログイン時の動作について、図２に示すフローチャートを参照しつつ説明する。

【００２７】まず、あらかじめ、この部屋（オフィス１）に入室可能な人物（利用者）の登録を、入退室登録装置７から入退室管理サーバ６を経由して、入室側制御装置９および退室側制御装置１０にそれぞれ行なう。登録されるのは、たとえば、ＩＤカードの場合であればＩＤ番号、指紋照合の場合は本人の指紋照合用データである。

【００２８】さて、いま入室を許可されたＡさんがオフィス１に入室したとする。その入室許可の判定結果は、入室側制御装置９から入退室管理サーバ６に送られ、Ａさんはオフィス１に正常入室状態と記憶される。この後、Ａさんはオフィス１内の所定のコンピュータ４からログイン名を入力し、ログインを行なおうとすると、コンピュータ４内のログイン管理プロセス（プログラム）は、それを検知することにより、直接ログイン管理サーバ２に認証にいくのではなく、入退室管理サーバ６内に当該ログイン名を持つ人が、自身のコンピュータのある部屋（ここではオフィス１）に正常入室状態であるかを確認に行く。

【００２９】具体的には、入退室管理サーバ６内には、Ａさんのログイン名があらかじめＡさんと対応付けられて登録されているため、そのログイン名からＡさんを検索し、Ａさんの入退室状態を検索する。なお、コンピュータ４内には、あらかじめ、どの部屋に設置されているのかの情報を記憶させておくか、コンピュータ名に設置場所名を付加しておくこととする。この情報から、ログイン管理プロセスは、コンピュータ４が設置されているオフィス１に正常入室状態であれば、次のステップとしてログイン管理サーバ２に対してログイン処理を依頼する。ここでは、ログイン名とパスワード（暗証番号）が確認され、その内容が正しければ正常にログインが許可される。

【００３０】Ａさんが作業を終え、ログアウトを行なうと、ログイン管理プロセスは、それを検知することにより、ログイン管理サーバ２に対してログアウト処理を依頼する。次に、Ａさんが退室すると、退室側制御装置１０から退室情報が入退室管理サーバ６へ送られ、Ａさんの状態は退室状態になる。

【００３１】ここで、たとえば、不正に入室した別人がＡさんのログイン名とパスワードを入手し、ログインを試みると、上記したように、ログイン管理プロセスは、最初に入退室管理サーバ６にＡさんの入退室状態を確認に行くが、この場合、Ａさんは退室状態にあるため、次のログイン管理サーバ２への処理に行かず、ログインできないこととなる。すなわち、コンピュータ４へのログインを拒否するものである。

【００３２】このような不正ログインの試みが行なわれると、ログイン管理プロセスは、その旨を入退室管理サーバ６へ通知し、入退室管理サーバ６内に記録として残すとともに、入退室管理サーバ６のディスプレイ６ａで警報表示し、警告を促す。

【００３３】次に、第２の実施の形態について説明する。

【００３４】前述した第１の実施の形態では、入退室管理サーバ６への入退室状態の確認をコンピュータ４内のログイン管理プロセスが行なったが、第２の実施の形態は、入退室管理サーバ６への入退室状態の確認をログイン管理サーバ２内のログイン管理プロセスが行なうようにしたものであり、その動作の流れを図３のフローチャートに示す。この場合、コンピュータ４のログイン管理プロセスの動きは全く変えることなく、ログインの依頼を受けたログイン管理サーバ２内のログイン管理プロセスが、ログイン許可の条件として、一般的である登録されたログイン名とパスワード、コンピュータ名に加えて、ログイン名から判断される利用者の入退室状態が正常入室状態になっていることを確認することで実現されるもので、その他は第１の実施の形態と同様である。

【００３５】次に、第３の実施の形態について説明する。

【００３６】図４は、第３の実施の形態に係る電子機器管理システムの構成を示すものである。第３の実施の形態の前述した第１の実施の形態と異なる点は、オフィス１の出入口８のみではなく、各コンピュータ４にも、それぞれ正当な利用者であるか否かを確認する個人確認装置（ＩＤカードであればＩＤカードリーダを用いたもの、指紋であれば指紋照合装置を用いたもの）１２を設置した点にあり、その他は第１の実施の形態と同様である。この場合、出入口８に設置された入退室制御装置９，１０と異なる確認方法の組合わせが、より高いセキュリティを確保する意味では有効である。たとえば、出入口８の入退室制御装置はＩＤカードによる確認方法を用い、コンピュータ４ごとの個人確認装置１２は指紋照合による確認方法を用いる。

【００３７】この第３の実施の形態の場合の動作の流れを図５のフローチャートに示す。この場合、コンピュータ４側のログイン管理プロセスは、個人確認装置１２を使用して、本人自身がアクセスしているかを確認後、個人確認装置１２から読取られた個人を特定する情報（たとえば、ＩＤカードであればＩＤ番号、指紋照合であれば指紋情報と１対１に意味付けられたＩＤ番号）をログイン名として、入退室管理サーバ６に入室状態を問い合わせ、正常入室状態にあった場合だけ、ログイン管理サーバ２に対してログイン処理を依頼する。

【００３８】なお、個人確認装置１２で用いるパスワード（暗証番号）は、キーボードからの入力を使用するか、または、指紋照合の場合は指紋情報の一部または全部を使用してもよい。

【００３９】このように、コンピュータ４側のログイン管理プロセスに処理を追加した場合は、既存のログイン管理サーバ２のプログラムに手を加える必要がなく、簡便にシステムを強化できる利点がある。また、入退室状態を確認することにより、入室許可のない部屋からのコンピュータアクセスが禁止できるため、アクセスをする場所といった物理的な制限を加えることが可能となる。

【００４０】さらに、この場合、何らかの方法で個人確認装置１２が不正な手段によって突破された場合でも、入退室管理側のデータを更にチェックすることにより、不正なログインを未然に防止することができる。

【００４１】以上説明したように、上記実施の形態によれば、オフィス１内に設置された複数のコンピュータ４へのログイン時、ログインの条件に、ＩＤカードや指紋照合などを用いた入室側制御装置９による、利用者が正常に当該コンピュータ４の設置されたオフィス１内に入室しているという条件を加えて判断し、正常に入室している場合にだけログインを許可し、正常に入室していない場合にはログインを拒否することにより、入室許可のない人の侵入によるコンピュータ４へのログインを排除することが可能となる。また、物理的な場所を特定してコンピュータ４からのログインの制限が可能となる。また、各コンピュータ４に個人確認用機器がない場合でも、上記作用効果を安価に実現できる。さらに、２つ以上の個人識別を組合わせることにより、不正なアクセス防止の効果をより高めるといった効果がある。

【００４２】なお、前記実施の形態では、オフィス内に設置された複数のコンピュータの利用を管理する場合について説明したが、本発明はこれに限定されるものではなく、たとえば、計測機器や医療機器など、他の電子機器の利用を管理する場合にも同様に適用できる。

【００４３】

【発明の効果】以上詳述したように本発明によれば、入室許可のない人の侵入による電子機器の利用を排除することができ、セキュリティを著しく向上させることができる電子機器管理システムおよび電子機器管理方法を提供できる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る電子機器管理システムの構成を模式的に示す構成図。

【図２】第１の実施の形態に係る基本的なログイン時の動作について説明するフローチャート。

【図３】第２の実施の形態に係る基本的なログイン時の動作について説明するフローチャート。

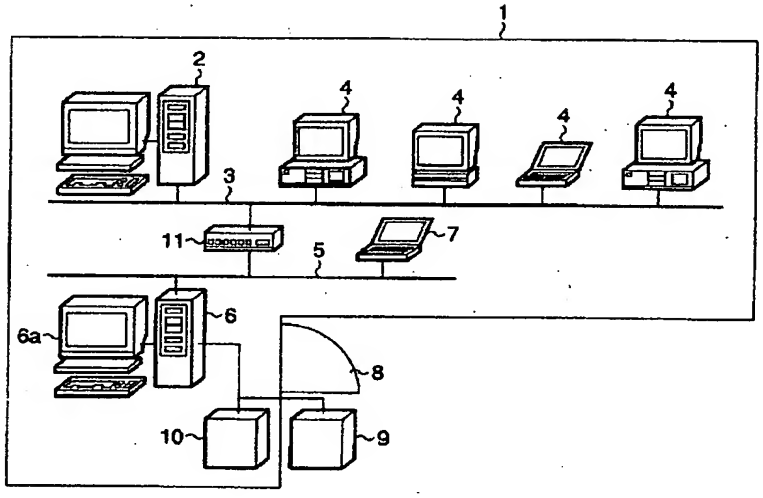
【図４】本発明の第３の実施の形態に係る電子機器管理システムの構成を模式的に示す構成図。

【図５】第３の実施の形態に係る基本的なログイン時の動作について説明するフローチャート。

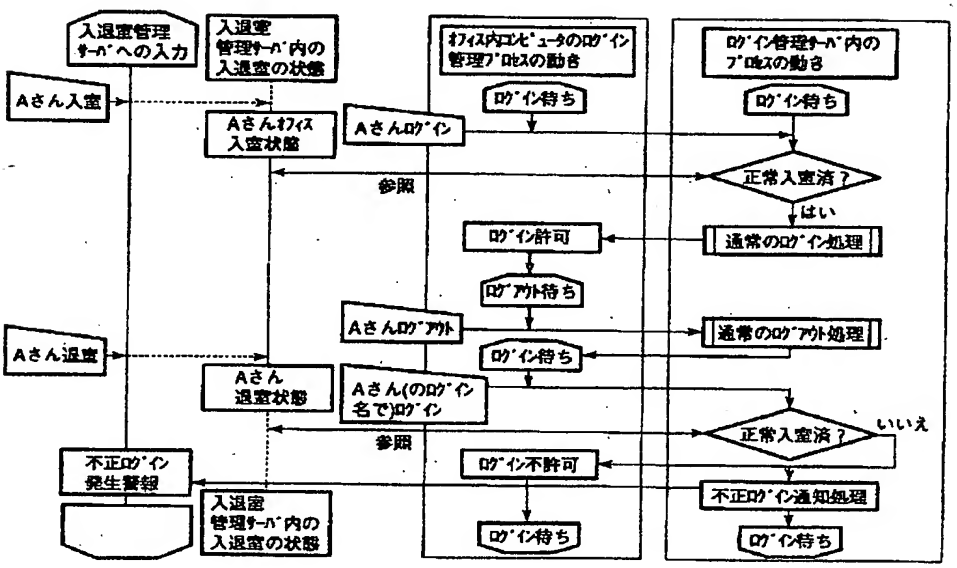
【符号の説明】

１…オフィス（部屋）
２…ログイン管理サーバ
４…コンピュータ（電子機器）
６…入退室管理サーバ
７…入退室登録装置
８…出入口
９…入室側制御装置
１０…退室側制御装置
１２…個人確認装置

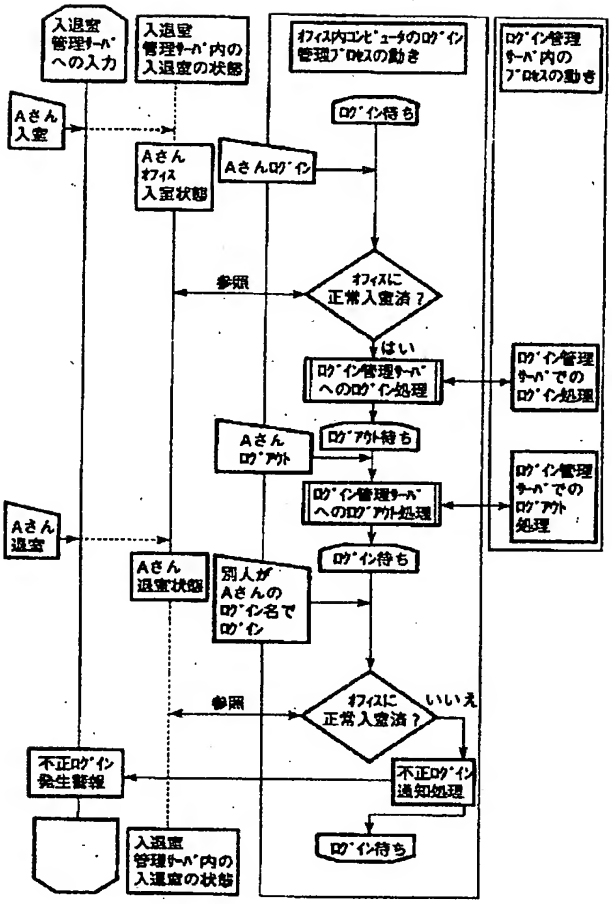
【図１】



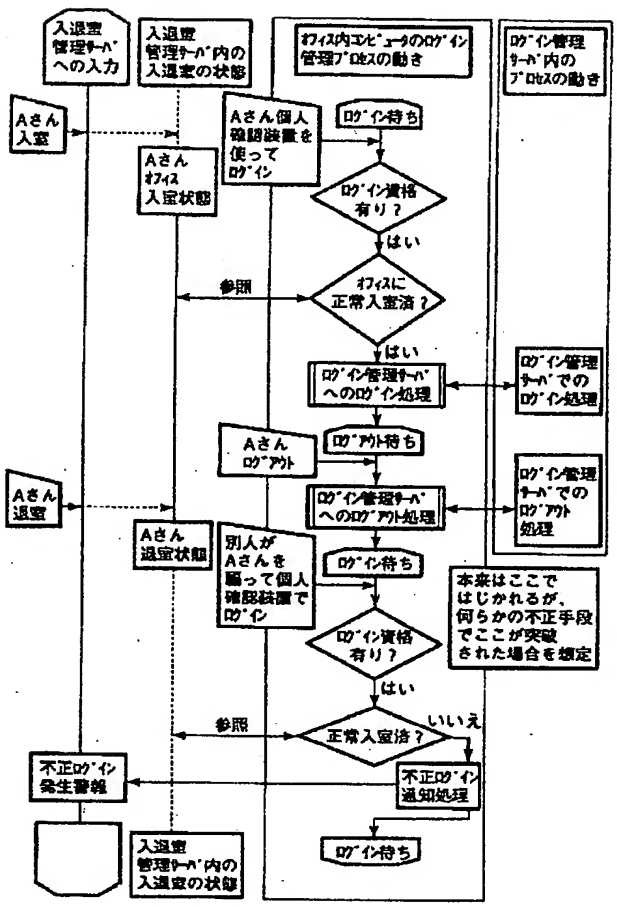
【図３】



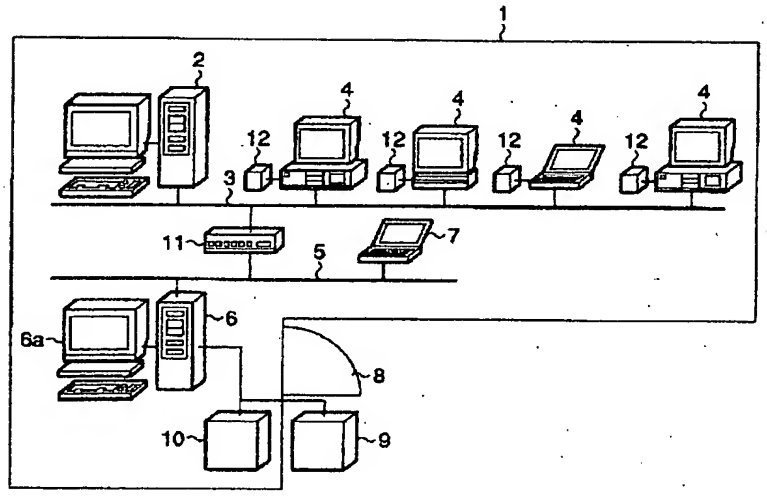
【図２】


入退室管理ｻｰﾊﾞへの入力
入退室管理ｻｰﾊﾞ内の入退室の状態
ｵﾌｨｽ内ｺﾝﾋﾟｭｰﾀのﾛｸﾞｲﾝ管理ﾌﾟﾛｾｽの動き
ﾛｸﾞｲﾝ管理ｻｰﾊﾞ内のﾌﾟﾛｾｽの動き
Aさん入室
Aさんｵﾌｨｽ入室状態
Aさんﾛｸﾞｲﾝ
ﾛｸﾞｲﾝ待ち
参照
ｵﾌｨｽに正常入室済？
はい
ﾛｸﾞｲﾝ管理ｻｰﾊﾞへのﾛｸﾞｲﾝ処理
ﾛｸﾞｲﾝ管理ｻｰﾊﾞでのﾛｸﾞｲﾝ処理
Aさんﾛｸﾞｱｳﾄ
ﾛｸﾞｱｳﾄ待ち
ﾛｸﾞｲﾝ管理ｻｰﾊﾞへのﾛｸﾞｱｳﾄ処理
ﾛｸﾞｲﾝ管理ｻｰﾊﾞでのﾛｸﾞｱｳﾄ処理
Aさん退室
Aさん退室状態
別人がAさんのﾛｸﾞｲﾝ名でﾛｸﾞｲﾝ
ﾛｸﾞｲﾝ待ち
参照
ｵﾌｨｽに正常入室済？
いいえ
不正ﾛｸﾞｲﾝ発生警報
不正ﾛｸﾞｲﾝ通知処理
ﾛｸﾞｲﾝ待ち
入退室管理ｻｰﾊﾞ内の入退室の状態

【図５】


入退室管理ｻｰﾊﾞへの入力
入退室管理ｻｰﾊﾞ内の入退室の状態
ｵﾌｨｽ内ｺﾝﾋﾟｭｰﾀのﾛｸﾞｲﾝ管理ﾌﾟﾛｾｽの動き
ﾛｸﾞｲﾝ管理ｻｰﾊﾞ内のﾌﾟﾛｾｽの動き
Aさん入室
Aさんｵﾌｨｽ入室状態
Aさん個人確認装置を使ってﾛｸﾞｲﾝ
ﾛｸﾞｲﾝ待ち
ﾛｸﾞｲﾝ資格有り？
はい
参照
ｵﾌｨｽに正常入室済？
はい
ﾛｸﾞｲﾝ管理ｻｰﾊﾞへのﾛｸﾞｲﾝ処理
ﾛｸﾞｲﾝ管理ｻｰﾊﾞでのﾛｸﾞｲﾝ処理
Aさんﾛｸﾞｱｳﾄ
ﾛｸﾞｱｳﾄ待ち
ﾛｸﾞｲﾝ管理ｻｰﾊﾞへのﾛｸﾞｱｳﾄ処理
ﾛｸﾞｲﾝ管理ｻｰﾊﾞでのﾛｸﾞｱｳﾄ処理
Aさん退室
Aさん退室状態
別人がAさんを騙って個人確認装置でﾛｸﾞｲﾝ
ﾛｸﾞｲﾝ待ち
本来はここではじかれるが、何らかの不正手段でここが突破された場合を想定
ﾛｸﾞｲﾝ資格有り？
はい
参照
正常入室済？
いいえ
不正ﾛｸﾞｲﾝ発生警報
不正ﾛｸﾞｲﾝ通知処理
ﾛｸﾞｲﾝ待ち
入退室管理ｻｰﾊﾞ内の入退室の状態

【図４】


1
2
3
4
5
6
6a
7
8
9
10
11
12